Test Procedure for §170.302 (s) Integrity

This document describes the draft test procedure for evaluating conformance of complete EHRs or EHR modules to the certification criteria defined in 45 CFR Part 170 Subpart C of the Interim Final Rule (IFR) as published in the Federal Register on January 13, 2010. The document is organized by test procedure and derived test requirements with traceability to the normative certification criteria as described in the Overview document located at http://healthcare.nist.gov/docs/TestProcedureOverview_v1.pdf. These test procedures will be updated to reflect the certification criteria defined in the ONC Final Rule.

Note: This test procedure is scoped only to the criteria defined in 45 CFR Part 170 Subpart C of the Interim Final Rule (IFR) as published in the Federal Register on January 13, 2010. This test procedure will be updated to reflect updates to the criteria and standards as published in the ONC Final Rule. Questions about the criteria and standards should be directed to ONC.

Certification Criteria

§170.302(s) Integrity:
(1) In transit. Verify that electronic health information has not been altered in transit in accordance with the standard specified in §170.210(c)
(2) Detection. Detect alteration and deletion of electronic health information and audit logs, in accordance with the standard specified in §170.210(c).

Informative Test Description

This section provides an informative description of how the test procedure is organized and conducted. It is not intended to provide normative statements of the certification requirements.

This test evaluates the capability for a Complete EHR or EHR Module[1] to verify whether electronic health information has been altered while in transit using a secure hashing algorithm (SHA-1 or higher). This does not test the ability to transmit data outside of the EHR.   The Vendor supplies test data for this test.

This test procedure consists of two sections:

- Generate hash values – evaluates the capability to generate a hash value
  - The Tester generates two hash values for comparison using Vendor-supplied test data
  - The Tester modifies the Vendor-supplied test data set and generates a hash value for the modified data set

- Compare hash values – evaluates the capability to compare hash values to ensure the electronic health information has not been altered in transit

[1] Department of Health and Human Services, 45 CFR Part 170 Proposed Establishment of Certification Programs for Health Information Technology, Proposed Rule, March 10, 2010.

- The Tester compares the generated hash values
- The Tester determines if the hash values are the same or different depending on the data sets

REFERENCED STANDARDS

§170.210(c)	Regulatory Referenced Standard
Verification that electronic health information has not been altered in transit. Standard. A secure hashing algorithm must be used to verify that electronic health information has not been altered in transit. The secure hash algorithm (SHA) used must be SHA-1 or higher.	

NORMATIVE TEST PROCEDURES

Derived Test Requirements

DTR170.302.s – 1: Generate hash values

DTR170.302.s – 2: Compare hash values

DTR170.302.s.1 – 1: Generate hash values

Required Vendor Information

VE170.302.s – 1.01: The Vendor shall provide EHR documentation identifying the secure hash algorithm (e.g., SHA-1 or higher) used to provide the hash value

VE170.302.s – 1.02: The Vendor shall identify the EHR function(s) that are available to generate and read hash values

VE170.302.s – 1.03: The Vendor shall identify test data available for this test

Required Test Procedure:

TE170.302.s – 1.01: The Tester shall examine Vendor-provided EHR documentation to determine if the vendor-identified secure hashing algorithm used to provide the hash value is SHA-1 or higher

TE170.302.s – 1.02: Using the Vendor-identified EHR function(s), the Tester shall generate two hash values for the Vendor-supplied test data

Using the Vendor-supplied test data set, the Tester shall modify the test data

TE170.302.s – 1.03: Using the Vendor identified EHR function (s), the Tester shall generate a hash value for the modified test data set

TE170.302.s – 1.04: The Tester shall output and store the hash value for comparison

Inspection Test Guide

IN170.302.s – 1.01: Tester shall verify that the Vendor-identified secure hashing algorithm used to provide the hash value is SHA-1 or higher

IN170.302.s – 1.02: Tester shall verify that two hash values have been generated from the Vendor-supplied test data and that one hash value has been generated from the modified Vendor-supplied test data

DTR170.302.s – 2: Compare hash values

Required Vendor Information

- As defined in DTR170.302.s.1 – 1, no additional information is required

Required Test Procedure:

VE170.302.s – 2.01: The Tester shall compare the hash values generated in the Generate hash values test using the Vendor-supplied test data

VE170.302.s – 2.01: The Tester shall compare one hash value generated in the Generate hash value test using the Vendor-supplied test data and the hash value generated using the modified Vendor-supplied test data

Inspection Test Guide

IN170.302.s – 2.01: Tester shall verify that the hash values are the same for the Vendor-supplied test data

IN170.302.s – 2.02: Test shall verify that the hash values are different for the modified Vendor-supplied test data

TEST DATA

Test data for this test procedure is supplied by the Vendor.

CONFORMANCE TEST TOOLS

None